U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-48 August 19, 2024

FINAL REPORT

CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

August 19, 2024

MEMORANDUM FOR: Troy A. Miller
Senior Official Performing the Duties of the Commissioner
U.S. Customs and Border Patrol

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.08.19 17:53:41 -04'00'

SUBJECT: *CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist*

Attached for your action is our final report, *CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving pre-arrival vetting procedures and mitigating vulnerabilities with the CBP One™ application. Your office concurred with all three recommendations.

Based on information provided in your response to the draft report, we consider all three recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGInspectionsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Thomas Kait, Deputy Inspector General for the Office of Inspections and Evaluations, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist

August 19, 2024

Why We Did This Evaluation

On January 12, 2023, CBP implemented the CBP One™ Advance Submission and Appointment Scheduling functionality allowing noncitizens to schedule appointments at select Southwest Border POEs. We conducted this evaluation to assess whether CBP adequately planned and implemented the CBP One™ application to process noncitizens who arrive at the Southwest Border.

What We Recommend

We made three recommendations to CBP to improve pre-arrival vetting procedures and mitigate vulnerabilities with the CBP One™ application.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

Although U.S. Customs and Border Protection (CBP) responded to CBP One™ application weaknesses after implementation, it did not formally assess and mitigate the technological risks involved with expanding the application to allow undocumented noncitizens (noncitizens) to schedule appointments to present themselves for processing at Southwest Border Ports of Entry (POEs). We found that CBP did not initially consider critical factors such as the design of the CBP One™ Genuine Presence functionality, adequacy of supporting application infrastructure, sufficiency of language translations, and equity of appointment distribution. As a result, noncitizens initially using the new feature experienced application crashes, received frequent error messages, faced language barriers, and may not have always had an equal opportunity to secure an appointment.

Additionally, CBP may be missing an opportunity to use CBP One™ advance information to improve pre-arrival vetting procedures. Although CBP uses biographic and biometric information submitted to CBP One™ to determine whether arriving noncitizens have derogatory records, it does not leverage the information to identify suspicious trends as part of its pre-arrival vetting procedures. Based on our analysis of CBP One™ data, we identified potentially unrelated noncitizens who repeatedly claimed identical U.S. residences as their intended address. CBP currently does not have a mechanism to routinely analyze CBP One™ data submitted across the eligible POEs for trends, which may be useful intelligence to help guide front-line CBP officers when interviewing noncitizens during appointment processing.

Finally, we identified security vulnerabilities within the CBP One™ application and its supporting infrastructure operating systems. Without a process to ensure all corrective security patches are timely implemented and assets are properly configured, CBP One™ data could be susceptible to exploitation or cyber-attacks. This process is especially important as CBP continues to update the application.

CBP Response

CBP concurred with all three recommendations. We consider all recommendations resolved and open.

Table of Contents

Abbreviations

ATA	Advance Travel Authorization
ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CDC	Centers for Disease Control and Prevention
CIS	Center for Internet Security
CM	Configuration Management
CRA	Cybersecurity Risk Assessment
EST	Eastern Standard Time
GAO	U.S. Government Accountability Office
IP	Internet Protocol
NTA	Notice to Appear
NTC	National Targeting Center
OFO	Office of Field Operations
OIT	Office of Information Technology

POA&M	Plan of Action and Milestones
POE	Port of Entry
SBOC	Southwest Border Operations Cell
TVS	Traveler Verification Service
UPAX	Unified Passenger
USEC	Unified Secondary System

Background

U.S. Customs and Border Protection (CBP) is charged with safeguarding our Nation's borders, including by ensuring all individuals entering the United States comply with applicable legal requirements. In October 2020, CBP developed the CBP One™ mobile and web application (CBP One™) to serve as a single portal for a variety of CBP services, such as applying for a Form I-94,[1] scheduling agricultural inspections at airports, and requesting Advance Travel Authorizations (ATA).[2] On January 12, 2023, CBP expanded the CBP One™ application to implement the Advance Submission and Appointment Scheduling (Appointment) feature. The CBP One™ Appointment feature allows undocumented noncitizens (noncitizens) seeking admission into the United States to submit advance information and schedule appointments at one of eight ports of entry (POEs)[3] along the Southwest Border.

Generally, undocumented noncitizens are individuals who do not possess valid travel documents—like a travel visa or passport[4]—that allow them entry into the United States. CBP officers spend considerable time collecting information and processing noncitizens at POEs because they do not possess valid travel documents. Historically, CBP has not received advance information prior to the noncitizen's arrival at a land border POE that would assist with this process. However, the CBP One™ Appointment feature streamlines this process by providing CBP officers with advance biographic and biometric information intended to reduce the administrative burden of manually entering information into systems of record to conduct pre-arrival noncitizen vetting.

Initially, the CBP One™ Appointment feature only allowed noncitizens seeking an exception to the Centers for Disease Control and Prevention's (CDC) public health policy, referred to as Title 42,[5] to schedule an appointment. After Title 42 expired on May 11, 2023, the CBP One™ Appointment feature was available for all noncitizens seeking safe and orderly arrival to the United States through the eight Southwest Border POEs.

[1] Form I-94 is the Department of Homeland Security arrival and departure record electronically issued to travelers who are admitted to the United States, that is also used for adjusting status while in the United States or extending their status, among other uses.
[2] A full list of the CBP One™ features can be found on CBP's website (https://www.cbp.gov/about/mobile-apps-directory/cbpone).
[3] The eight POEs included Brownsville, Texas; El Paso, Texas; Eagle Pass, Texas; Hidalgo, Texas; Laredo, Texas; Calexico, California; San Ysidro, California; and Nogales, Arizona.
[4] 8 C.F.R. § 212.1, *Documentary requirements for nonimmigrants*.
[5] On March 20, 2020, the CDC announced the Public Health Order *Suspending Introduction of Certain Persons from Countries Where a Communicable Disease Exists*. Pursuant to Sections 362 and 365 of the Public Health Service Act, 42 United States Code (U.S.C.) §§ 265, 268, CDC's Order suspended the introduction of persons into the United States from countries where a quarantinable communicable disease exists. CBP is authorized to except individuals from the CDC Order on a case-by-case basis, to include for humanitarian reasons.

CBP processed 264,554 noncitizens who registered with CBP One™ between January 12, 2023, and August 18, 2023, and secured an appointment at one of the eligible POEs prior to September 28, 2023. Figure 1 depicts the distribution of the CBP One™ appointments across the eight eligible Southwest Border POEs. Of those, CBP officers processed at least 237,533 (89.8 percent)[6] noncitizens with a Notice to Appear (NTA).[7] Per CBP POE officials, CBP officers typically process CBP One™ appointment holders who do not present a public safety risk with an NTA; these noncitizens receive up to a 2-year parole into the United States while they await their immigration court hearing date.

Figure 1. CBP One™ Appointments Distribution by POE

Source: DHS Office of Inspector General analysis of CBP One™ registration data

Overview of CBP One™ Appointment Processing

The CBP One™ appointment process is composed of three distinct phases: appointment scheduling, pre-arrival vetting, and POE processing. The following narrative describes the initial processes when CBP first launched the CBP One™ Appointment feature on January 12, 2023.

[6] We could not locate disposition records for 22,041 of 264,554 (8 percent) noncitizens with a CBP One™ appointment.

[7] Form I-862, *Notice to Appear*, is an official charging document that places a noncitizen into removal proceedings before an immigration judge.

Appointment Scheduling (noncitizen)

Starting at 9 a.m. Eastern Standard Time (EST) each day, noncitizens could access the CBP One™ mobile application to create a registration and submit advance information. To register for CBP One™, noncitizens must have established a Login.gov[8] account using a personal email address, which is a security feature that authenticates a person's identity. As shown in Figure 2, noncitizens would input their biographical information into CBP One™, such as their name, date of birth, country of birth, intended U.S. residence, etc.[9] Additionally, noncitizens had to submit a photograph that was subject to CBP's Genuine Presence[10] technology to verify the user was a "live" person. CBP's Traveler Verification Service (TVS) gallery utilizes all photographs submitted into CBP One™ to assist with verifying noncitizens during POE processing. Noncitizens could register multiple people under the same registration, which allowed families to request appointments together. CBP One™ also captured the device's latitude and longitude to ensure the noncitizen was within the appropriate proximity to the U.S. border to schedule an appointment.[11] If an appointment was available, noncitizens could select an appointment location and time immediately after completing the registration process. When CBP initially released the CBP One™ Appointment feature, noncitizens could schedule appointments up to 14 days in advance.

Figure 2. Example of CBP One™ Advance Information Screen

Source: CBP One™ Application

Pre-Arrival Vetting Process (POE)

After a noncitizen scheduled an appointment, CBP One™ registration information was stored in the Automated Targeting System (ATS). Functionality within ATS, called Unified Passenger (UPAX), automatically conducted pre-arrival vetting by comparing noncitizen-provided information against other data available to CBP, such as raw intelligence from DHS and other Government agencies. Using this information, UPAX automatically generated a CBP One™ Hotlist for each POE, which documented all upcoming appointments and pre-arrival vetting results.

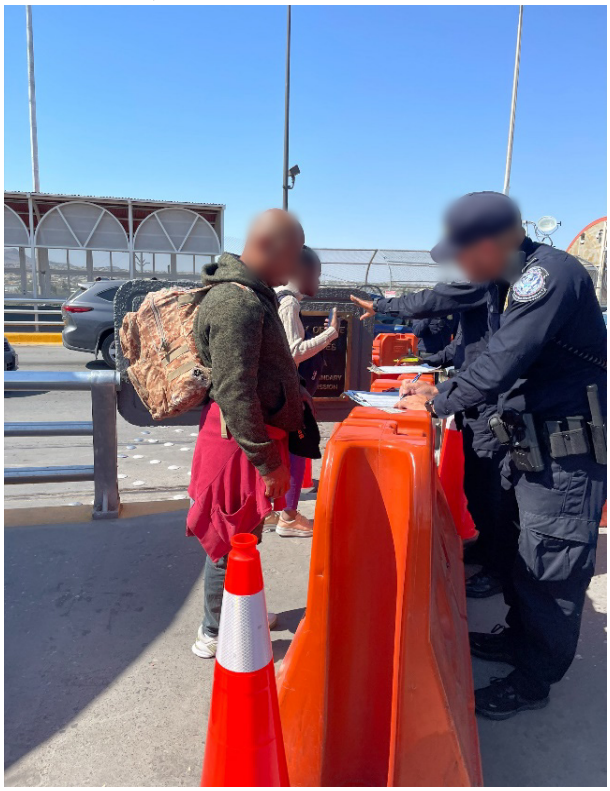
[8] Login.gov is a secure sign-in service used by the public to sign in to participating Government agencies to securely access information.
[9] CBP One™ registration collects the same biographic information that is otherwise collected at the POE upon arrival.
[10] The Genuine Presence technology uses the camera on the user's device to authenticate the user is a real person.
[11] Users need to be located north of Mexico City, Mexico to schedule CBP One™ appointments.

Additionally, CBP's Southwest Border Operations Cell (SBOC),[12] created the "CBP One Appointment Holders of Interest Report" to notify senior officials, including POE Directors of Field Operations, of noncitizens scheduled to arrive in the next 72 hours who posed a potential national security concern.[13] POEs used both reports to assist with screening noncitizens, and ran additional queries on criminal history databases before their arrival, as necessary. If POEs identified arriving noncitizens with a potentially derogatory record, CBP officers created an "event" in UPAX that allowed the National Targeting Center (NTC) to assist with vetting after the individual arrived for their appointment.

Appointment Processing (POE)

On the day of their appointment, noncitizens arrived at the POE for processing. As shown in Figure 3, CBP officers used the CBP One™ Hotlist to verify noncitizens had a confirmed appointment prior to entering the POE. Once verified, CBP officers' directed noncitizens into the POE to begin primary inspection. At primary inspection, CBP officers collected biometric information, including a photograph for comparison to the TVS gallery to retrieve the noncitizens' advance information in CBP One™ and pre-populate CBP's Unified Secondary (USEC)[14] system. Noncitizens were then referred to secondary processing where CBP officers confirmed the advance information submitted into CBP One™, collected the noncitizen's fingerprints for comparison to the Department's Automated Biometric Identification System—known as IDENT—for a criminal background check, collected a DNA sample that they provide to the Federal Bureau of Investigations for Combined DNA Index System processing, reviewed vetting results, and coordinated with the NTC to confirm derogatory information, as necessary. At any time during processing, CBP officers could have interviewed or asked

Figure 3. CBP Officers Verifying CBP One™ Appointments at Limit Line Observed on October 18, 2023

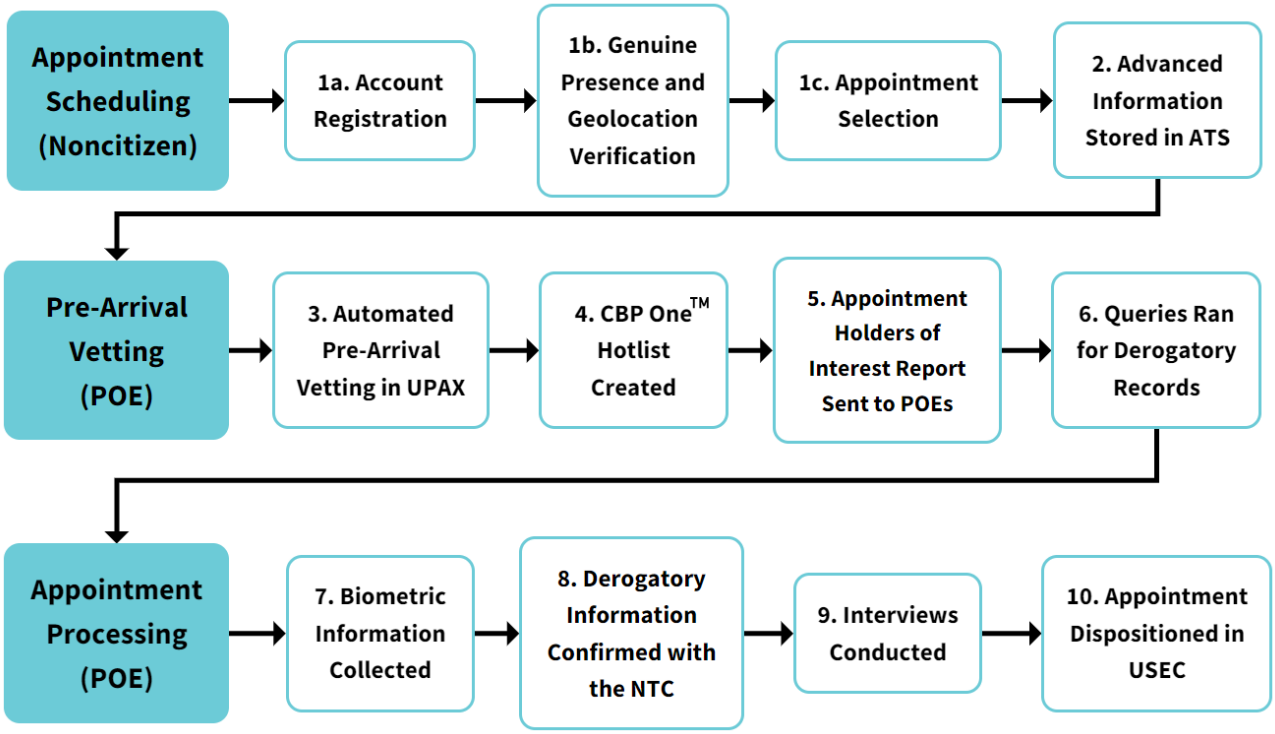


Source: DHS OIG photograph taken at the El Paso POE

[12] The SBOC is a temporary detachment from CBP's Office of Field Operation's (OFO) Incident Response Division, which oversees all activity related to field operations.
[13] In this context, national security concern is defined as an individual who has a potential match to a Terrorist Screening Database or Transnational Organized Crime record.
[14] USEC is a module within CBP's ATS that serves as a system to consolidate secondary processing actions from referral to resolution

additional questions to noncitizens who presented a possible risk. Using the totality of this information, CBP officers determined the appropriate processing of each noncitizen, which is recorded in the USEC system.[15] Figure 4 depicts the flow of the initial processes when CBP first launched the CBP One™ Appointment feature on January 12, 2023.

Figure 4. CBP One™ Initial Appointment Scheduling thru POE Processing (January 12, 2023 - February 22, 2023) Flowchart



Source: DHS OIG analysis of CBP One™ initial appointment processes

Between January and May 2023, CBP made two significant updates to the application that changed how noncitizens scheduled appointments. On February 23, 2023, CBP separated the account registration process from the appointment selection process so that noncitizens scheduled appointments separately from creating an account registration. Additionally, on May 10, 2023, CBP transitioned from a first-come, first-served appointment selection model to an algorithm-based appointment allocation model.[16] Appendix C depicts the evolution of the CBP One™ registration and appointment scheduling processes at these three critical timeframes.

[15] We observed CBP One™ appointment processing at the El Paso POE, and these processes took several hours to complete.
[16] CBP allocates appointments daily based on a pool of those who requested an appointment. A percentage of those selected are reserved for those with the oldest registrations and the remaining appointments are selected randomly.

We conducted this evaluation to assess whether CBP adequately planned and implemented the CBP One™ application to process noncitizens who arrive at the Southwest Border.

Results of Evaluation

Although CBP responded to CBP One™ weaknesses after implementation, it did not formally assess and mitigate the technological risks involved with expanding the application to allow noncitizens to schedule appointments to present themselves for processing at the Southwest Border. We found that CBP did not initially consider critical factors such as the design of the CBP One™ Genuine Presence functionality, adequacy of supporting application infrastructure, sufficiency of language translations, and equity of appointment distribution. As a result, noncitizens initially using the new feature experienced application crashes, received frequent error messages, faced language barriers, and may not have always had an equal opportunity to secure an appointment.

Additionally, CBP may be missing an opportunity to use CBP One™ advance information to improve pre-arrival vetting procedures. Although CBP uses biographic and biometric information submitted into CBP One™ in advance to determine whether arriving noncitizens have derogatory records, it does not leverage the information to identify suspicious trends as part of its pre-arrival vetting procedures. Based on our analysis of CBP One™ data, we identified potentially unrelated noncitizens who repeatedly claimed identical intended U.S. residences. CBP currently does not have a mechanism to routinely analyze CBP One™ data submitted across the eligible POEs for trends, which may be useful intelligence to help guide front-line CBP officers when interviewing noncitizens during appointment processing.

Finally, we identified security vulnerabilities within the CBP One™ application and its supporting infrastructure operating systems. Without a process to ensure all corrective security patches are timely implemented and assets are properly configured, CBP One™ data could be susceptible to exploitation or cyber-attacks. This process is especially important as CBP continues to update the application.

CBP Did Not Assess and Mitigate Critical Technological Risks Prior to Implementing the CBP One™ Appointment Feature

CBP did not conduct a formal risk assessment[17] to mitigate critical technological risks prior to expanding the CBP One™ application. Per the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book), Federal entities should identify, analyze, and respond to risks related to achieving defined objectives. Specifically,

[17] Risk assessment is the identification and analysis of risks related to achieving the defined objectives.

management should consider the types of internal and external risks that impact the entity, including the use of new technology in operational processes. We found that CBP did not formally assess and mitigate the technological risks involved with expanding CBP One™ to meet its new operational objective of scheduling appointments for noncitizens to arrive at the Southwest Border. Performing a risk assessment may have allowed CBP to initially consider critical factors such as the design of the CBP One™ Genuine Presence functionality, adequacy of supporting application infrastructure, sufficiency of language translations, and equity of appointment distribution as described below.

CBP Did Not Thoroughly Plan the CBP One™ Genuine Presence Functionality

CBP did not adequately plan for or design the CBP One™ Genuine Presence functionality, which is a security feature designed to verify the application user is a real person. Noncitizens who use the CBP One™ Appointment feature to schedule appointments must submit a photograph for processing by software to verify "genuine presence," or that the user is a live person. This is a critical security feature to ensure CBP One™ users are real individuals and not bad actors[18] using a fraudulent identity to obtain an appointment.

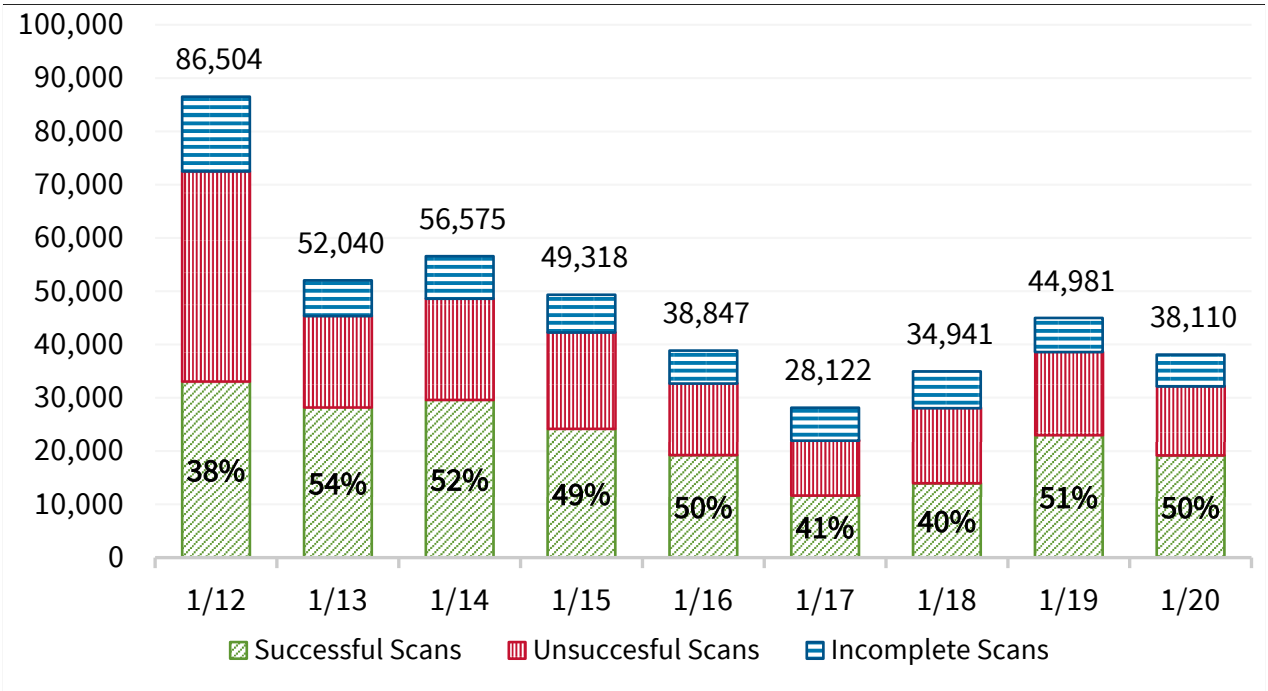
CBP uses third-party software to verify genuine presence through a contract with a technology company specializing in biometric verification and authentication. The initial contract obligated the contractor to conduct a maximum of 400,000 scans between August 19, 2022, and November 18, 2023, with a maximum rate of 1 scan per second. However, as shown in Figure 5, the contractor conducted 429,438 scans in the first 9 days the CBP One™ Appointment feature was operational, per the contractor's activity reports. When the CBP One™ Appointment feature launched on January 12, 2023, the contractor processed 86,504 scans on the first day of operation alone. Further, milestone reports show that it processed up to 32 scans per second on January 12, 2023, which exceeded the contractor's obligation of a maximum of 1 scan per second.

CBP officials told us that it did not anticipate the unprecedented demand for CBP One™ appointments, which depleted the contracted number of scans within days of initial public launch. Furthermore, CBP did not warn the contractor of the expected increase in the number of CBP One™ users before it launched the Appointment Feature. Consequently, the contractor did not initially implement a control to limit the rate of Genuine Presence scans it could process per second. Once the CBP One™ demand was identified, the contractor throttled, or reduced, the number of scans it processed per second to align with contractual requirements. However, this effectively increased the rate of rejected scans, which caused noncitizens using the application to receive error messages. As shown in Figure 5, the Genuine Presence scans were successful

[18] Bad actor is defined as a person, group, or country who purposely engages in bad behavior, such as committing a crime.

only 38 percent of the time on January 12, 2023, which highlights the frequency noncitizen's received error messages.

Figure 5. Genuine Presence Transactions, January 12-20, 2023



Source: DHS OIG summary of third-party contractor activity report data

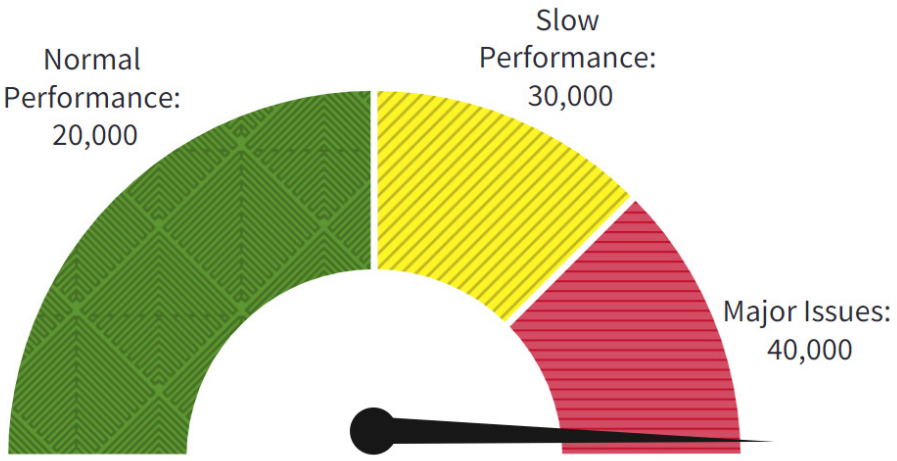
Further, CBP's inefficient design of the Genuine Presence feature further exacerbated the rapid depletion of available scans. CBP originally designed the CBP One™ Appointment feature to include a Genuine Presence scan every time a noncitizen attempted to schedule an appointment, even if an appointment was unavailable. According to a contractor Milestone Report, multiple user attempts to access the application resulted in a "high level of wastage" of limited Genuine Presence scans, which showed the importance of conducting the scans only after an appointment was available. As a result, this was an inefficient use of the limited Genuine Presence scans available to support the CBP One™ Appointment feature.

CBP took several steps to mitigate this issue after implementation. On February 17, 2023, CBP modified its contract to increase the number and rate of Genuine Presence scans the contractor could conduct. Additionally, on February 23, 2023, CBP separated the registration and appointment scheduling processes, which more effectively allocated its available Genuine Presence scans. After this CBP One™ update took effect, noncitizen photographs were only subject to a Genuine Presence scan if an appointment was available, which improved the overall CBP One™ service. See Appendix C for a summary of the appointment process change that took effect on February 23, 2023.

CBP Did Not Implement an Adequate CBP One™ Infrastructure

CBP did not implement an adequate infrastructure to support the increase in CBP One™ traffic from noncitizens using the application to schedule appointments at the Southwest Border. In December 2022, prior to CBP implementing the Appointment feature, CBP conducted a load test on the application, which found that it could handle up to 20,000 transactions[19] every 5 minutes, or 240,000 transactions every hour, without an issue. According to the load test results, CBP One™ would start to slow-down when processing 360,000 transactions per hour and would experience major issues when processing 480,000 transactions per hour. On January 12, 2023—the Appointment feature's first day of operation—more than 449,000 unique CBP One™ users attempted to use the application. According to CBP Office of Information Technology (OIT) officials, this total does not account for noncitizens who made multiple requests (i.e., refreshing the application), which created further strain on the system. Furthermore, many of these users attempted to access CBP One™ at the same time—9 a.m. EST— in preparation for the release of new appointment timeslots. CBP OIT officials confirmed that the volume of CBP One™ traffic caused extreme strain on its infrastructure, as shown in Figure 6.

Figure 6: CBP One™ User Traffic on January 12, 2023, at 9 a.m. EST



Source: DHS OIG Analysis of CBP One™ load test results and CBP One™ usage data

The unexpected number of noncitizens concurrently accessing CBP One™ combined with the decision to funnel CBP One™ access to 9 a.m. EST ultimately overwhelmed its underlying infrastructure, resulting in low bandwidth and users receiving error messages. CBP's OIT promptly responded to these issues by upgrading CBP One™ processing power on January 13th, January 20th, and again on March 15th. Each of these upgrades improved CBP One™ bandwidth

[19] A transaction is a business scenario in the application that is being tested, such as logging into the application.

and overall performance. Additionally, on May 10, 2023, CBP modified the appointment request process, which eliminated the daily login time to request an appointment, effectively reducing the initial behaviors that overloaded the system. See Appendix C for a summary of the appointment process change that took effect on May 10, 2023.

CBP Did Not Provide Sufficient CBP One™ Language Support

CBP did not sufficiently translate the CBP One™ Appointment feature to enable noncitizens using the application to schedule appointments. When CBP initially implemented the new Appointment feature on January 12, 2023, it was available in English and partially in Spanish.[20] CBP later added translation support for the Haitian-Creole language on February 1, 2023, based on stakeholder feedback.[21] Our analysis of CBP One™ registration data shows that only 66,128 of the 113,239 (58 percent) noncitizens who used the Appointment Feature between January 12, 2023, and January 31, 2023, could use the application in their primary language.[22] Table 1 illustrates the primary languages of the noncitizens who created CBP One™ registrations during this period.

Table 1. CBP One™ Primary Languages through January 31, 2023

Primary Language	No. of Registrations	Percentage	Cumulative Percentage	Available in CBP One™?
Spanish	65,352	57.7%	57.7%	Yes
English	776	0.7%	58.4%	Yes
Haitian-Creole	26,429	23.3%	81.7%	No*
Russian	15,051	13.3%	95.0%	No
Others	5,631	5%	100%	No
Total	**113,239**	**100%**		

* CBP added Haitian-Creole language support on February 1, 2023.

Source: DHS OIG analysis of CBP One™ registration data

CBP continued to improve translation services to the CBP One™ Appointment feature after its initial implementation. For example, as previously noted, on February 1, 2023, CBP translated application error messages to Haitian-Creole. Additionally, CBP One™ terms and conditions were initially only available in English. Noncitizens are required to accept the terms and conditions to use the application, which includes pertinent information such as the acknowledgment of providing personally identifiable information and the penalties for intentionally making false

[20] CBP did not initially translate CBP One™ terms and conditions and drop-down menus in Spanish.
[21] CBP One™ stakeholders that provided application feedback included non-governmental organizations and users of the application.
[22] Noncitizens provide their preferred language during the CBP One™ registration process.

statements. On April 6, 2023, CBP translated CBP One™ terms and conditions to Spanish and Haitian-Creole. Finally, CBP translated the information contained in CBP One™ drop-down menus—such as date of birth, gender, and country of citizenship—to Spanish and Haitian-Creole on May 10, 2023.

According to a CBP Office of Field Operations (OFO) official, CBP did not initially translate the CBP One™ Appointment feature in Haitian-Creole because it prioritized translating the CBP One™ ATA feature to Haitian-Creole. CBP became aware in December 2022 that individuals from Haiti would be eligible for humanitarian parole under the separate Cubans, Haitians, Nicaraguans, and Venezuelans[23] process, which relies on the CBP One™ ATA feature. Additionally, a CBP OIT official stated they initially provided error messages in Spanish and translating them to other languages impacted how the application could store information. To mitigate this issue, OIT later created a workaround that successfully allowed the application to translate error messages. As of February 2024, the CBP One™ appointment scheduling feature remains available in only English, Spanish, and Haitian-Creole, which as shown in Table 1, does not support all application users.

CBP Did Not Ensure Equitable Distribution of CBP One™ Appointments

CBP did not take sufficient steps to prevent the misuse of CBP One™ registrations to gain an advantage in securing an appointment. As noted in the background, noncitizens must first create a CBP One™ registration before requesting an appointment. Based on our analysis of CBP One™ registration data, we found 52,992 of the 1,336,401 (4 percent) noncitizens who created a registration between January 12, 2023, and August 18, 2023, created at least 10 unique registrations. As shown in Table 2, many of these noncitizens created hundreds of unique registrations that resulted in a CBP One™ appointment. According to CBP OFO officials, creating multiple registrations is one fraudulent tactic used to increase noncitizens' probability of securing a CBP One™ appointment.

[23] Noncitizens from Cuba, Haiti, Nicaragua, and Venezuela may use the CBP One™ ATA feature to request advance travel authorization to the United States to seek parole.

Table 2. Top 10 Individuals Who Submitted Multiple CBP One™ Registrations and Secured a CBP One™ Appointment

Individual	Citizenship	April	May	June	July	Total
Individual 1	Armenian	-	-	466	-	466
Individual 2	Armenian	-	-	466	-	466
Individual 3	Armenian	-	-	466	-	466
Individual 4	Russian	-	1	432	-	433
Individual 5	Armenian	-	-	360	-	360
Individual 6	Armenian	-	-	321	-	321
Individual 7	Russian	-	-	312	-	312
Individual 8	Russian	-	-	312	-	312
Individual 9	Armenian	-	111	197	-	308
Individual 10	Armenian	-	-	293	-	293

Source: DHS OIG analysis of CBP One™ registration data

When CBP initially implemented the Appointment feature on January 12, 2023, a limited number of daily appointments were available on a first-come, first-served basis; and noncitizens were required to access the application at 9 a.m. EST each day.[24] Creating multiple registrations under these circumstances was potentially advantageous when individuals were included in more than one group registration. According to a CBP OFO official, they identified instances where individuals in a group of noncitizens each created a CBP One™ registration that contained all individuals in the group, which increased each individual's chance of securing an appointment before another noncitizen.

Creating multiple registrations was even more effective after May 10, 2023, when CBP modified the process of distributing appointments in response to stakeholder feedback. With this modified process, noncitizens no longer had to access the application at the same time each day to schedule an appointment. Instead, the application added noncitizens who requested an appointment to an applicant pool and CBP's algorithm[25] distributed appointments, as detailed in Appendix C.

As shown in Table 2, we found that the noncitizens who most used this tactic to obtain an appointment perpetuated this scheme in the May and June timeframe, which aligned with the timing of CBP's appointment allocation method update. CBP officials confirmed that using this tactic to create multiple registrations increased some noncitizens' chances of securing

[24] CBP initially allocated 1,000 appointments per day and gradually increased the number of daily appointments to 1,450.
[25] A percentage of noncitizens with the oldest registrations will be selected from the appointment pool. The remaining appointments are selected randomly.

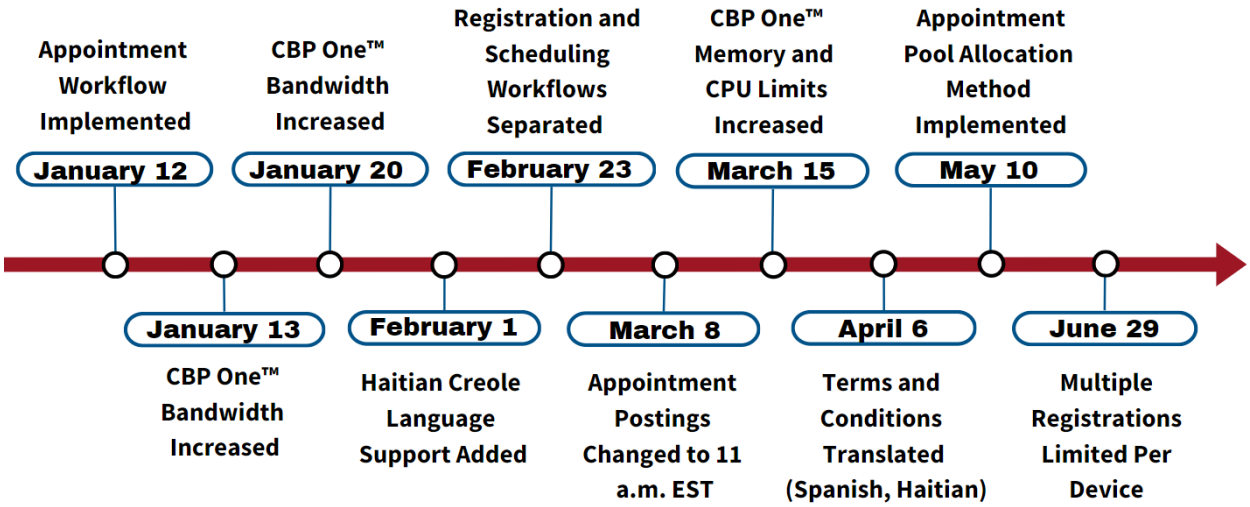
appointments while simultaneously decreasing the chances for other users. Further review of timestamp data revealed that some of these noncitizens created registrations within a few seconds of each other on the same date, which is impossible to legitimately accomplish given the registration information requirements. According to a CBP OFO official, these individuals may have used bots or scripts to create their registrations and apply for appointments.

While the CBP One™ update on May 10, 2023, addressed bandwidth issues, it may have further incentivized the use of fraudulent tactics to create duplicate registrations and obtain an appointment. To combat this, on June 29, 2023, CBP implemented a control that limits the number of CBP One™ registrations per device. Although CBP implemented corrective actions to mitigate the impact of creating multiple registrations, noncitizens who used the CBP One™ application prior to the update did not have an equal opportunity to obtain an appointment.

CBP One™ Updates After Implementation

Although CBP did not conduct a formal risk assessment prior to expanding the CBP One™ application, we found CBP responded to weaknesses after they implemented the application. As shown in Figure 7 and discussed in detail in the preceding sections of this report, CBP made numerous technical updates to the CBP One™ Appointment feature since its initial implementation on January 12, 2023. Generally, CBP made the updates to improve application performance, increase access to its features, and combat fraudulent tactics. According to a CBP OFO official, CBP used feedback it received from CBP One™ stakeholders to improve the application.

Figure 7. Timeline of Significant CBP One™ Application Updates (2023)



Source: DHS OIG summary of significant CBP One™ updates

Despite CBP's efforts to apply mitigating controls after they implemented the CBP One™ Appointment feature, noncitizens who initially used the new feature experienced application crashes, received frequent error messages, and faced language barriers. Additionally, noncitizens may not have always had an equal opportunity to secure an appointment because of inadequate controls over registration creation. CBP may have avoided these issues if it had conducted a formalized risk assessment before implementing the CBP One™ Appointment feature.

CBP Did not Maximize its Use of CBP One™ Advance Information

Although CBP used information submitted through CBP One™ to conduct pre-arrival noncitizen vetting at individual POEs, it missed an opportunity to assess the advance information for trends of suspicious activity across the Southwest Border and communicate results to POEs for consideration during admissibility determinations. CBP's *Privacy Impact Assessment for the Collection of Advance Information from Certain Undocumented Individuals on the Land Border* (January 19, 2023), states that one of the objectives of CBP One™ is to gain efficiencies with processing individuals by gathering advance information prior to their arrival. Obtaining advance information allows CBP to perform pre-arrival vetting against existing databases and identify trends of suspicious activity.

Based on our review of CBP One™ data, we found suspicious trends in the noncitizens' pre-reported U.S. residential address, which is a required field during the CBP One™ registration process. For example, we found that 208,996 of 264,554 noncitizens (79 percent) who registered in CBP One™ between January 12, 2023, and August 18, 2023,[26] reported the same intended residence as another noncitizen despite appearing to be unrelated.[27] As shown in Table 3, we identified seven U.S. addresses that 1,696 noncitizens claimed as their intended residence, which we considered suspicious and potentially relevant to their admissibility determinations.[28] Furthermore, the 1,696 noncitizens did not enter into the United States through the same POEs.

[26] This statistic refers to noncitizens who registered between this period and secured a CBP One™ appointment prior to September 28, 2023.
[27] CBP One™ data does not identify whether groups of individuals are related. Instead, we used unique last names to measure individuals who were potentially unrelated.
[28] In OIG-23-47, *DHS Does Not Have Assurance That all Migrants Can be Located Once Released into the United States*, we reported a similar finding involving migrants who provided addresses to U.S. Border Patrol agents that may pose unsafe or overcrowded living conditions once they are released from custody.

Table 3. Seven Most Frequently Reported U.S. Residences, by POE

Port of Entry	Address 1	Address 2	Address 3	Address 4	Address 5	Address 6	Address 7	Total
San Ysidro	261	247	188	50	56	67	53	**922**
Brownsville	85	44	38	82	13	9	10	**281**
Hidalgo	33	38	21	62	37	25	11	**227**
Calexico	26	8	17	4	13	15	13	**96**
Laredo	14	5	9	11	6	4	5	**54**
Eagle Pass	5	5	8	16	0	4	6	**44**
El Paso	11	6	1	23	1	1	0	**43**
Nogales	6	5	4	9	0	2	2	**28**
Total	**441**	**358**	**286**	**257**	**126***	**127**	**100**	**1,695***

* We identified one additional noncitizen processed without a POE designated in the CBP One™ dataset.

Source: DHS OIG analysis of CBP One™ registration data

In one particularly striking example, we identified 358 noncitizens who reported the same 4-bedroom, single-family home (Address 2 in Table 3) as their intended U.S. residence within an 8-month period. Of the 358 noncitizens, we identified 266 noncitizens with different last names who were potentially unrelated to one another. As shown in Figure 8, the 358 noncitizens who reported the same intended residence entered through any one of the eight POEs along the Southwest Border. As a result, no single POE realized the number of noncitizens reporting this suspicious address.

Figure 8. Example of Noncitizens Route to a Suspicious U.S. Residence (Address 2 in Table 3), by POE Origin

Source: DHS OIG analyses of CBP One™ data.

CBP does not have a mechanism to routinely analyze CBP One™ advance information for suspicious trends across the eight Southwest Border POEs as part of its pre-arrival vetting procedures. Specifically, individual POEs only have access to the biographic and biometric information of noncitizens who make appointments at their location. Additionally, CBP's SBOC Division was not tasked with analyzing CBP One™ advance information for suspicious trends. However, it does regularly communicate with POEs to notify them of arriving noncitizens who pose potential national security threats. Finally, the NTC assists the POEs with tracking and vetting noncitizens after they arrive for their appointment, but it does not vet CBP One™ advance information prior to their arrival.

Additionally, CBP considers the CBP One™ data to be unvalidated, and therefore unreliable, until the POEs can confirm the noncitizen's identity after they arrive for their appointment. According to CBP OFO officials, noncitizens can change their residence address when they arrive at the POE. Our analysis of disposition data from the USEC system shows that 83 percent of the suspicious addresses we identified in CBP One™, shown in Table 3, were the same addresses used in the

noncitizen's Form I-862, *Notice to Appear*,[29] which CBP completes as part of appointment processing at the POE. Therefore, we believe that U.S. residences reported in CBP One™ may be sufficiently reliable for trend analysis purposes.

CBP may be missing an important opportunity to leverage CBP One™ advance information to help inform front-line CBP officers of trends across all eligible POEs. An analysis of trends could be a valuable tool to help guide targeted noncitizen interviews during POE processing, which could potentially uncover and disrupt national security threats, such as human trafficking or other illicit activities.

Security Vulnerabilities Exist within the CBP One™ Application and Supporting Infrastructure Operating Systems

CBP generally complied with CBP One™ database security requirements. However, we identified security vulnerabilities within the CBP One™ application and its supporting infrastructure.[30] We conducted a code review of the CBP One™ mobile application and a vulnerability assessment of the CBP One™ web application. Additionally, we performed compliance and vulnerability scans against the underlying databases and supporting infrastructure operating systems to determine whether security risks exist. Based on the results of our assessments, we identified vulnerabilities within the CBP One™ mobile application, web application and supporting infrastructure operating systems that could compromise the integrity of sensitive systems and information.

CBP One™ Mobile Application Vulnerabilities

The public facing CBP One™ mobile application has software weaknesses that could compromise its system access controls. Noncitizens can use the mobile application to submit advance information and schedule CBP One™ appointments. As shown in Table 4, our review of the application's code revealed five instances[31] of one unique[32] high-risk[33] vulnerability.

---

[29] Per 8 U.S.C. § 1229, written notice of removal proceedings must be given to any person not a citizen or national of the United States that indicates the time and place of their legal proceedings and an address at which they can be contacted.

[30] On May 15, 2023, DHS OIG Office of Audits initiated an audit of CBP's Mobile Device Management and Security to determine the extent to which CBP manages and secures its mobile devices.

[31] Instances refers to the number of times a particular vulnerability was identified and quantifies the total threat to the system.

[32] Unique refers to the number of different individual vulnerabilities and highlights the number of Component remediation activities required to mitigate or reduce the identified vulnerability.

[33] Risk ratings are determined by the mobile application scan tool by considering the impact and likelihood of successful exploitation of an identified vulnerability. High vulnerabilities can lead to major security issues and are important to remediate.

Table 4. CBP One™ Mobile Application Vulnerability Assessment Results

Security Vulnerability	High-Risk	Critical-Risk
Instances	5	0
Unique	1	0

Source: DHS OIG Cybersecurity Risk Assessment (CRA) Division vulnerability testing results

Specifically, the "Missing Google Play Services Updated Security Provider" vulnerability for Android device users indicates that the application is not using the latest security features provided by Google Play Services.[34] This can lead to potential security risks, such as exposure to known vulnerabilities and weakened encryption,[35] compromising the application's overall security and potentially putting user data at risk.

Per DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems* (DHS 4300A),[36] components implement controls to protect the information received by DHS information systems. DHS 4300A requires components to, "employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within DHS information systems." Given the identified vulnerabilities, it appears CBP has not applied all necessary controls to protect information submitted into the CBP One™ mobile application.

CBP One™ Web Application Vulnerabilities

The CBP One™ web application has a software weakness making its security controls susceptible to bypass. The desktop application is accessible via a web browser,[37] which noncitizens can use to create CBP One™ registrations and submit associated advanced biographic information.[38] As shown in Table 5, our vulnerability assessment revealed five instances of one unique medium-risk[39] software weakness. Specifically, bad actors could use the weakness identified to bypass

[34] The Google Play Services Security Provider is a set of security services and updates provided by Google Play Services that enhance the security of Android applications.
[35] Data encryption translates data from unencrypted text to encrypted text to defend against cyber-attacks.
[36] DHS 4300A establishes the information security policy for DHS based on federal security regulations.
[37] https://cbpone-cert.cbp.dhs.gov/#/.
[38] Only the CBP One™ mobile application can be used to schedule an appointment because a mobile device is required to meet geolocation requirements.
[39] Risk ratings are vendor-defined within the web application scan tool. This determination is made by considering the impact of successful exploitation in a typical application.

front-end security rules, access internal systems, and potentially launch attacks on users who are actively browsing the website.

Table 5. CBP One™ Web Application Vulnerability Assessment Results

Security Vulnerability	Low-Risk	Medium-Risk	High-Risk
Instances	0	5	0
Unique	0	1	0

Source: DHS OIG CRA Division vulnerability testing results

Per DHS 4300A, DHS shall conduct periodic vulnerability assessments of DHS information systems to determine security risks that should be mitigated. Additionally, the directive states that a Plan of Action and Milestone (POA&M)[40] must be generated for identified weaknesses within 145 days of its discovery. However, CBP was not aware of the vulnerability before we conducted our assessment. Therefore, it had not developed a POA&M to correct the deficiency, as required.

CBP One™ Infrastructure Operating System Patch Management

The CBP One™ application is deployed as a containerized environment that resides on the underlying infrastructure.[41] CBP did not timely implement all patches intended to mitigate CBP One™ server vulnerabilities in accordance with DHS remediation timeframes. Patches ensure operating systems, such as CBP One™ infrastructure operating systems, keep pace with new and emerging vulnerabilities. As shown in Table 6, we found 22 unique high-risk vulnerabilities, and 1 unique critical-risk vulnerability existing within the infrastructure operating systems that support the CBP One™ application.[42] In particular, the vulnerabilities identified make CBP One™ infrastructure operating systems susceptible to information disclosure and denial-of-service attacks.[43]

[40] A POA&M is a plan designed to correct deficiencies and reduce or eliminate vulnerabilities in DHS information systems.
[41] Containerization is a software deployment process that bundles an application's code with all the files and libraries it needs to easily run with limited external dependencies.
[42] The scan tool assigns all vulnerabilities a severity (Info, Low, Medium, High, or Critical) based on the vulnerability's Common Vulnerability Scoring System score, which is a free and open industry standard for assessing the severity of computer system security vulnerabilities.
[43] A denial-of-service attack is a cyber-attack that seeks to prevent access to a network by flooding the server with traffic.

Table 6. CBP One™ Infrastructure Operating Systems Patch Management Vulnerability Assessment Results

Security Vulnerability	Low-Risk	High-Risk	Critical-Risk
Unique	0	22	1

Source: DHS OIG CRA Division vulnerability testing results

DHS 4300A requires that information security patches are installed in accordance with the timeframes published by the DHS Enterprise Security Operations Center.[44] According to CBP OIT officials, the CBP One™ infrastructure has a 5-week patching schedule during which patches are tested and deployed. We found that CBP did not timely implement all security patches to mitigate the identified infrastructure security vulnerabilities.

CBP One™ Infrastructure Operating System Configuration Management

CBP did not implement all required configuration management (CM)[45] settings, or have approved waivers, critical to maintaining the security of the CBP One™ application. We assessed the CBP One™ infrastructure operating systems against CBP's chosen CM standard, known as the Center for Internet Security's (CIS) Benchmark Level 1 (L1) and Level 2 (L2)[46] baselines, as well as its chosen Defense Information Systems Agency Security Technical Implementation Guide[47] and best practice security configurations. As shown in Table 7, we found that CBP did not implement 2,281 of the 12,388 (18.4 percent) L1 CM settings and did not implement 526 of the 5,124 (10.3 percent) L2 CM settings.

[44] The DHS Enterprise Security Operations Center coordinates security operations for the DHS enterprise. Each component also has a Security Operations Center that coordinates Component security operations.
[45] CM is the act of managing the configuration of all hardware and software elements of information systems and networks, which has a direct impact on the security of the system.
[46] CIS Level 1 benchmarks are considered less intrusive, base recommendations, while Level 2 benchmarks are considered defense-in-depth, more security focused recommendations.
[47] The Defense Information Systems Agency developed the Security Technical Implementation Guides, which include configuration standards to make device hardware and software as secure as possible.

Table 7. CBP One™ Infrastructure Operating System Configuration Management Vulnerability Assessment Results

CIS Benchmark	CM Settings Failed	CM Settings Tested	Percentage
L1	2,281	12,388	18.4%
L2	526	5,124	10.3%

Source: DHS OIG CRA Division vulnerability testing results

For example, we found that CBP did not ensure internet protocol (IP) forwarding was disabled on CBP One™ infrastructure, which is a CM L1 recommended setting. IP forwarding can be subject to cybersecurity threats, and attackers can exploit it to gain unauthorized access if implemented incorrectly or with inadequate security measures. Additionally, improper configuration of IP forwarding can consume significant bandwidth and potentially impact network performance. Further, we found CBP did not ensure it tracked system actions that modify system access, which is a CM L2 recommended setting. Tracking of these types of system actions could identify if an unauthorized user attempts to modify access controls, potentially leading to system compromise.

It is critical for Federal agencies to have CM programs in place to implement secure settings that prevent threat actors from exploiting vulnerable configurations and services. According to CIS, default configurations for operating systems and applications are normally geared towards ease-of-deployment instead of focused on security. For example, basic controls, default accounts or passwords, and pre-installation of unneeded software can all be exploited in their default state. Therefore, it is critical for CBP to implement strong CM practices to increase the security of CBP One™ systems and information.

Without implementing timely corrective security patches and required configuration settings, CBP One™ data could be susceptible to potential exploitation and expose the confidentiality, integrity, and availability of information to bad actors. As CBP One™ is a public-facing application, it is imperative that CBP continually manage security settings to avoid security "decay" as CBP updates or patches software, identifies new security vulnerabilities, and installs new software to support operational requirements. As shown in Figure 7, CBP applied numerous technical updates to the CBP One™ application to meet operational demands and respond to threats. This highlights the importance of timely implementing patches and configuration management settings as software evolves.

Conclusion

The CBP One™ Appointment feature was not fully ready to fulfill its purpose—to streamline the POE experience and facilitate a safe and orderly arrival for noncitizens—when CBP implemented it in January 2023. Although CBP promptly applied controls to mitigate CBP One™ weaknesses after its implementation, it did not conduct a formalized risk assessment prior to the application's expansion. As a result, noncitizens using the application when it was first introduced experienced application crashes, received frequent error messages, faced language barriers, and may not have always had an equal opportunity to secure an appointment.

Additionally, CBP may be missing an important opportunity to leverage CBP One™ information to identify suspicious trends across the eight Southwest Border POEs. Historically, CBP has not received advance information about noncitizens prior to their arrival at POEs. The introduction of CBP One™ changes that and could allow CBP to conduct and supply POE officers with trend analyses to enhance their ability to identify and disrupt national security threats, such as human trafficking.

Finally, security vulnerabilities within the CBP One™ application and its supporting infrastructure operating systems could compromise the security of CBP One™ information. Without a process to ensure all corrective patches are timely implemented and assets properly configured, CBP One™ data could be at risk of exploitation.

Recommendations

Recommendation 1: We recommend CBP's Office of Field Operations develop and implement a formalized risk assessment process when developing, expanding, or modifying mobile applications.

Recommendation 2: We recommend CBP's Office of Field Operations implement a mechanism to analyze CBP One™ advanced information for trends and patterns of fraudulent behaviors by users of CBP One™ and communicate its results to the eight ports of entry that process CBP One™ appointments.

Recommendation 3: We recommend CBP's Office of Information Technology implement a mechanism to routinely assess CBP applications and supporting infrastructure operating systems for configuration and patch management vulnerabilities and timely implement corrective actions.

Management Comments and OIG Analysis

CBP provided written comments in response to the draft report and concurred with all three recommendations. Appendix B contains CBP's management comments in their entirety. We also received technical comments from CBP on the draft report and revised the report as appropriate. We consider all three recommendations resolved and open. A summary of CBP's response and our analysis follows.

CBP Response to Recommendation 1: Concur. CBP's Innovation Center will incorporate a formal risk assessment when developing or modifying mobile applications. This will be in the form of a document that notes the risks considered for each developed or modified mobile application and the plans to mitigate the risks. The estimated completion date for actions needed to close this recommendation is October 31, 2024.

OIG Analysis of CBP's Comments: These actions are responsive to the recommendation, which we consider resolved and open. We will close the recommendation when CBP provides documentation to substantiate it has implemented a formal risk assessment process.

CBP Response to Recommendation 2: Concur. CBP began ingesting CBP One™ advance information data elements into its Analytical Framework for Intelligence system on March 21, 2024. The ingestion of this data makes it immediately available for authorized CBP users including CBP's Office of Intelligence, field analytical elements, front-line officers, and agents. Additionally, CBP's National Targeting Center will conduct analysis to identify trends and patterns of potential fraudulent behaviors by users of CBP One™ and develop a mechanism to communicate the results to the ports of entry that process CBP One™ appointments. The estimated completion date for actions needed to close this recommendation is October 31, 2024.

OIG Analysis of CBP's Comments: These actions are responsive to the recommendation, which we consider resolved and open. We will close this recommendation when CBP provides documentation to substantiate it has implemented a mechanism to analyze CBP One™ information for trends and patterns of fraudulent activity and communicate its results to the ports of entry that process CBP One™ appointments.

CBP Response to Recommendation 3: Concur. All applications running on the CBP managed Kubernetes environment were migrated to the Cloud provider-managed Kubernetes platform by March 29, 2024, including CBP One™. CBP considers the infrastructure operating system patch resolved as of April 10, 2024. Additionally, CBP's OIT will establish a process for reviewing and mitigating CBP application vulnerabilities and validate the remediation of the identified vulnerabilities with updated scans. The estimated completion date for actions needed to close this recommendation is September 30, 2024.

OIG Analysis of CBP's Comments: These actions are responsive to the recommendation, which we consider resolved and open. We will close this recommendation when CBP provides documentation to substantiate it has established a process for reviewing and mitigating CBP application vulnerabilities and provides updated vulnerability scans that validate remediation.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this evaluation to assess whether CBP adequately planned and implemented the CBP One™ application to process noncitizens who arrive at the Southwest Border.

To achieve our objective, we conducted 11 interviews with personnel from CBP's OFO, OIT, Privacy Office, NTC, Front Office, and several POEs to understand their roles with the development and implementation of the CBP One™ Appointment feature. We also observed CBP One™ appointment processing at the El Paso POE, in El Paso, Texas, in October 2023.

Additionally, we obtained noncitizen registration data submitted into CBP One™ between January 12, 2023, and August 18, 2023. This dataset included the CBP One™ appointment date if the registration resulted in an appointment prior to November 13, 2023. We also obtained disposition event data from the USEC system between April 22, 2022, and September 27, 2023.

To analyze the adequacy of CBP's planning of the CBP One™ Appointment feature, we examined all noncitizen registration data submitted into CBP One™ between January 12, 2023, and August 18, 2023. Specifically, we analyzed noncitizen primary language data to determine the sufficiency of CBP One™ translations. Additionally, we examined the number of noncitizen registrations to determine the extent noncitizens created multiple registrations that could impact appointment allocations.[48] Finally, we examined technical documentation, such as third-party contracts and milestone reports, CBP One™ load test results, CBP One™ usage data, and application version history, to determine the adequacy of CBP One™ bandwidth and the supporting technical infrastructure.

To analyze the adequacy of CBP's implementation of the CBP One™ Appointment feature, we examined noncitizen registration data submitted into CBP One™ between January 12, 2023, and August 18, 2023, with a confirmed appointment prior to September 28, 2023. We restricted the scope of this analysis to appointment dates prior to September 28, 2023, so that we could isolate noncitizens who had a confirmed appointment and identify the associated disposition recorded in the USEC system. Specifically, we reviewed the CBP One™ registration data to identify trends

[48] CBP One™ noncitizen registration information did not contain a unique noncitizen identifier, such as a Social Security number. To quantify the number of registrations per noncitizen, we created a unique field that consisted of first name, last name, and date of birth.

of suspicious activity and reviewed the USEC disposition data to determine the outcome of each CBP One™ appointment.

Finally, we coordinated with the DHS OIG Office of Innovation's CRA Division to conduct security assessments of the CBP One™ application and supporting infrastructure to determine whether security risks exist. DHS OIG's CRA Division supports OIG audits, evaluations, and inspections with information technology Security expertise, technical systems testing, vulnerability assessments, and information technology security controls reviews for protection of DHS data and infrastructure. Specifically, CRA conducted a code review of the CBP One™ mobile application, a vulnerability assessment of the CBP One™ web application, and compliance and vulnerability scans against the underlying databases and infrastructure operating systems.

We conducted this evaluation between August 2023 and January 2024 under the authority of the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this evaluation, CBP denied the OIG's request for direct, read-only access to the data contained within the CBP One™ system. In lieu of system access, CBP provided the OIG with all requested data extracts.

Appendix B:
CBP Comments on the Draft Report

1300 Pennsylvania Avenue, NW
Washington, DC 20229
U.S. Customs and Border Protection

July 23, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph. D.
Inspector General
Office of Inspector General

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

7/23/2024

SUBJECT: Management Response to Draft Report: "Evaluation of CBP's Implementation of CBP One™ for Southwest Border Undocumented Noncitizens" (Project No. 23-033-ISP-CBP)

Thank you for the opportunity to comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CBP takes pride in its organizational commitment to promote accountability and facilitate lawful trade and travel at the more than 300 land, air, and sea ports of entry. CBP's core values are vigilance, service, and integrity. In fulfilling its law enforcement mission, CBP leadership demands the highest standards of honesty, impartiality, and professionalism. Detecting misuse and abuse of the CBP One™ application (CBP One™) and deploying countermeasures is a top priority for CBP.

CBP leadership appreciates the OIG's recognition of efforts to respond to challenges posed by the urgent expansion of CBP One™, a mobile application that was quickly designed to allow undocumented noncitizens seeking an exception to the Centers for Disease Control and Prevention's public health policy (also known as Title 42) to schedule an appointment. No time was available for a formal assessment of technical risks prior to implementation given the unprecedented demand for appointments during the initial CBP One™ rollout. However, CBP has made significant improvements and continues to strengthen the application to address risk-related issues and concerns. For example, in May 2023, CBP reengineered the appointment allocation process to help mitigate technical difficulties that resulted from the initial implementation requiring all users to access the application at the same time each day. More specifically, CBP implemented a process that allots 12 hours for users to request appointments and up to 47 hours for users to confirm appointments. This

approach eliminated most connectivity issues experienced by users and provided a more predictable process with ample time to address any technical issues that may arise.

In addition, as of March 24, 2024, all advance information collected through CBP One™, including addresses and phone numbers, are now available to intelligence and CBP Officers for risk assessment and trend analysis, as appropriate, with the caveat that these data are self-reported and unverified.

CBP has also been diligent in combating the misuse of the application and potential exploitation of the noncitizen population through the monetization of services by bad actors to utilize an otherwise free application. As mentioned in the OIG's draft report, malicious actors sometimes attempt to gain appointments by using multiple registrations in a single day or bypassing geofence requirements to request an appointment. Since the OIG's fieldwork, CBP has implemented several measures to ensure equity in appointment allocations and compliance with geofence requirements. Key measures include: the implementation of the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) and encryption to identify and block scripts and emulators; deployment of security services to identify the use of "fake GPS" apps or altered devices; and the utilization of facial matching to identify duplicate registrations. When fraud is detected, CBP One™ sends users an error message that potential fraud was detected and deactivates their registrations. If a user believes their registration was deactivated in error, they can email the CBP One™ inbox at CBPOne@cbp.dhs.gov requesting a review to confirm the original finding of fraud.

It is also important to note that CBP One™ is an application designed for a mobile device (such as a smartphone) and is not a system of records used to store data. CBP *disagrees* with the OIG's assertion that CBP denied access to CBP One™ when CBP provided the needed datasets and answered related questions in a timely manner. More specifically, providing the OIG with access to the application would not have granted access to the datasets the OIG was seeking. Instead, CBP provided datasets responsive to the review in order to facilitate the OIG's work. In responding to the OIG requests for wholesale access to IT systems, CBP analyzes each request, considering, in part, whether the vast majority of data in a system is related to the scope and objectives of the OIG's review, as well as the types of sensitive information held in the system.

The draft report contained three recommendations with which CBP concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, sensitivity, contextual, and editorial issues under a separate cover for the OIG's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure

Enclosure: Management Response to Recommendations Contained in 23-033-ISP-CBP

OIG recommended that CBP's Office of Field Operations:

Recommendation 1: Develop and implement a formalized risk assessment process when developing, expanding, or modifying mobile applications.

Response: Concur. CBP's Innovation Center will incorporate a formal risk assessment when developing or modifying mobile applications. This will be in the form of a document that notes the risks considered for each developed or modified mobile application and the plans to mitigate the risks. Estimated Completion Date (ECD): October 31, 2024.

Recommendation 2: Implement a mechanism to analyze CBP One™ advanced information for trends and patterns of fraudulent behaviors by users of CBP One™ and communicate its results to the eight ports of entry that process CBP One™ appointments.

Response: Concur. On March 21, 2024, OFO began ingesting all CBP One™ advance data elements into the Analytical Framework for Intelligence system. The ingestion of this data makes it immediately available for authorized CBP users including but not limited to CBP's Office of Intelligence, field analytical elements and front-line officers, and agents. This data is a resource for conducting advance analysis on an individual basis as well as trend analysis. CBP's National Targeting Center will conduct analysis to identify trends and patterns of potential fraudulent behaviors by users of CBP One™ and develop a mechanism to communicate the results to the eight ports of entry that process CBP One™ appointments. ECD: October 31, 2024.

OIG recommended that CBP's Office of Information Technology (OIT):

Recommendation 3: Implement a mechanism to routinely assess CBP applications and supporting infrastructure operating systems for configuration and patch management vulnerabilities and timely implement corrective actions.

Response: Concur. All applications running on the CBP managed Kubernetes[1] environment were migrated to the Cloud provider managed Kubernetes platform by March 29, 2024, including CBP One™. CBP informed the OIG Cybersecurity Risk Assessment Division that it considers this infrastructure operating system patch resolved on April 10, 2024, and sent supporting documentation under separate cover on July 9, 2024. CBP's OIT will establish a process for review and mitigation of CBP application vulnerabilities found in web and container scans. OIT will also validate the remediation of the identified vulnerabilities with updated scans. ECD: September 30, 2024.

[1] Kubernetes is an open-source platform designed to automate the deployment, scaling, and operation of containerized applications (for example CBP One™).

Appendix C:
CBP One™ Registration and Appointment Scheduling Processes

Phase 1 Jan. 12, 2023, to Feb. 22, 2023 **Update:** Implemented Submit Advance Information Feature	Phase 2 Feb. 23, 2023, to May 9, 2023 **Update:** Registration and Scheduling Workflows Separated	Phase 3 May 10, 2023, through present **Update:** Implemented Appointment Pool Selection Method
Step 1. CBP One™ Registration thru Appointment Scheduling Starting at 9 a.m. EST each day, noncitizen creates a registration in CBP One™ and provides biographical information, including a photo that must meet Genuine Presence verification [photo added to TVS Gallery]. Noncitizen must be within prescribed proximity to the U.S. border to meet geolocation requirements. If an appointment is available, noncitizen selects day, time, and POE. If an appointment is unavailable, noncitizen must return later to access the previously created registration, provide new live photo, and pass geolocation check.	**Step 1. CBP One™ Registration** Noncitizen creates a registration in CBP One™ and provides biographical information for all members of group, including a photo [photo added to TVS Gallery]. Registration not restricted to geolocation requirements. **Step 2. Appointment Request** Starting at 9 a.m. EST each day [changed to 11 a.m. EST on March 8, 2023], noncitizen requests an appointment within CBP One™ at desired POE. **Step 3. Appointment Confirmation** If a timeslot is available for all members of group, registration owner submits a photo for Genuine Presence verification [photo added to TVS Gallery]. Photo is compared to prior photo submitted to verify the individual, and user must meet geolocation requirements. Next, noncitizens select day and time of desired appointment and receive a confirmation.	**Step 1. CBP One™ Registration** Noncitizen creates a registration in CBP One™ and provides biographical information for all members of group, including a photo [photo added to TVS Gallery]. Registration not restricted to geolocation requirements. **Step 2. Appointment Request** Between 12 p.m. and 11 a.m. EST (23-hour period) each day, noncitizen requests an appointment at desired POE. If user's device meets geolocation requirements, noncitizen is added to the appointment applicant pool. **Step 3. Appointment Allocation** Between 11 a.m. and 12 p.m. EST, the CBP One™ algorithm allocates appointments to noncitizens in the pool. Noncitizens who are not selected can ask for an appointment the next day. **Step 4: Appointment Confirmation** Noncitizens have 23 hours to confirm the appointment or can request a 23-hour extension. To confirm, a user on the registration must submit a photo for Genuine Presence verification [photo added to TVS Gallery] and meet geolocation requirements. Photo is compared to prior photo submitted to verify the individual. Once confirmed, noncitizens receive a confirmation.

Appendix D:
Major Contributors to This Report

John D. Shiffer, OIE, Chief Inspector
Michael Nasuti, OIE, Lead Inspector
Erika Algeo, OIE, Senior Inspector
Brett Cheney, OIE, Senior Inspector
Dorie Chang, OIE, Communications Analyst
Thomas Rohrback, OIN, Director
Jason Dominguez, OIN, Supervisory IT Cybersecurity Specialist
Joseph Sanchez, OIN, IT Specialist
Catlin O'Halloran, OC, Assistant Counsel to the Inspector General
Brendan Bacon, OIE, Independent Referencer

Appendix E:
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commissioner, CBP
Audit Liaison, CBP

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305